SALSEC
Companhia de Securitização de Salvador

Política de Segurança da Informação

2025

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

COMPANHIA DE SECURITIZAÇÃO DE SALVADOR – SALSEC

Política de Segurança da Informação

Responsável pela elaboração	Diretoria Executiva e Assessoria Jurídica
Responsável pela aprovação	Conselho de Administração
Datas da aprovação	29/09/2025
Versão	V.1

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1 OBJETIVO E FUNDAMENTOS

1.1. A informação é um patrimônio da SALSEC e ativo essencial para o cumprimento dos objetivos sociais da empresa.

1.2. A SALSEC reconhece o espaço cibernético como um recurso indispensável para a execução de suas estratégias de negócio.

1.3. A estratégia de segurança cibernética da SALSEC baseia-se na aplicação das melhores práticas para proteger o ecossistema de negócios, por meio de um programa de gestão do risco de segurança cibernética.

1.4. A Política de Segurança da Informação objetiva estabelecer diretrizes gerais, princípios e responsabilidades para garantir que as informações da SALSEC e de seus clientes sejam protegidas contra divulgação, modificação ou acesso não autorizados, por meio de ações voltadas a:

1.4.1. Assegurar que a segurança da informação e a segurança cibernética estejam integradas a todas as atividades e processos da SALSEC.

1.4.2. Administrar e reduzir os riscos de segurança da informação e segurança cibernética, fortalecendo a imagem da Empresa, e atendendo aos requisitos de negócios e exigências regulatórias e legais.

1.4.3. Estabelecer processos e implementar tecnologias que permitam à SALSEC identificar, prevenir, detectar e reduzir o risco cibernético.

2 PRINCÍPIOS

2.1 A SALSEC fundamenta seus processos e atividades nos seguintes princípios:

2.1.1 Segurança Operacional: as proteções implementadas devem possuir como principal premissa a salvaguarda e respeito à vida humana, garantindo que um incidente de segurança cibernética ou segurança da informação não se torne um acidente que possa causar danos à integridade física de pessoas.

2.1.2 Disponibilidade: as proteções implementadas devem considerar todos os requisitos que mantenham a disponibilidade de sistemas de informação imposta pela necessidade de negócio. Nenhuma medida de proteção implementada poderá comprometer a disponibilidade ou afetar o desempenho requerido pelo negócio.

2.1.3 Integridade: as proteções implementadas devem garantir a manutenção das condições iniciais das informações, de acordo com a forma com que foram produzidas e armazenadas.

2.1.4 Confidencialidade: as proteções implementadas devem ter como premissa a garantia de que a informação estará acessível apenas a pessoas autorizadas.

2.1.5 Aplicabilidade: os controles de segurança implementados supõem um procedimento exequível e uma estrutura compatível com a organização da SALSEC.

2.1.6 Monitoramento: os controles de segurança selecionados devem ser capazes de notificar qualquer evento suscetível a impactar o bom funcionamento ou a proteção dos sistemas de informação.

2.1.7 Rastreabilidade: os sistemas de informação devem possuir registros de ações realizadas, permitindo que seja possível identificar os responsáveis por elas, bem como o exato momento em que ocorreram.

3 Abrangência e Comprometimento da Alta Administração

3.1. A presente Política aplica-se à SALSEC, devendo ser observada por seus acionistas, administradores, empregados, investidores, representantes e parceiros, especialmente, mas não se limitando, àqueles que possuem poderes delegados de decisão, ou seja, os conselheiros, diretores, gerentes, assessores, coordenadores, membros de comitês e de comissões.

3.2. Todas as informações (em papel, digitais, áudio, vídeo), sistemas, serviços em nuvem, dispositivos e instalações sob gestão ou responsabilidade da SALSEC, inclusive ambientes de desenvolvimento, homologação e produção.

3.3. O Conselho de Administração, a Presidência e a Diretoria Executiva compreendem a importância da segurança da informação e segurança cibernética para a SALSEC e se comprometem para uma gestão efetiva das ações para identificar, mitigar e monitorar os riscos associados às ameaças cibernéticas e para que esta Política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização.

4 Processos

4.1. A SALSEC integra-se ao sistema oficial da Secretaria Municipal da Fazenda – SEFAZ, em observância à LGPD, e utiliza os processos abaixo descritos para assegurar que os controles de segurança sejam implementados e que as informações e os ativos cibernéticos possuam os níveis de proteção adequados:

a. Gestão de ativos: classificação dos ativos de Tecnologia da Informação (TI) e Tecnologia da Operação (TO), incluindo hardware e software, de acordo com a criticidade e objetivos da organização.

b. Gestão de vulnerabilidades: utilização de planos, procedimentos e tecnologias apropriadas para detectar, identificar, analisar, gerenciar e responder a vulnerabilidades e ameaças cibernéticas.

c. Gestão do risco cibernético: execução de processos para identificar, analisar e responder ao risco cibernético nos ambientes de Tecnologia da Informação (TI) e Tecnologia da Operação (TO).

d. Gestão de identidade e acesso: criação e gerenciamento de identidades para as entidades que acessem o ambiente SALSEC, com o controle de acesso baseado no menor privilégio, necessidade do negócio e segregação de papéis.

e. Tratamento de incidentes de segurança: utilização de planos, procedimentos e tecnologias para detectar, analisar, mitigar, responder e recuperar de incidentes de segurança cibernética e garantir a continuidade da operação dos serviços e sistemas da SALSEC.

f. Monitoramento: atividades e tecnologias para coletar, monitorar e analisar as comunicações de Tecnologia da Informação (TI) e de Tecnologia da Operação (TO) para estabelecer a capacidade de compreensão do ambiente em operação e a habilidade de resposta rápida.

g. Gestão de risco em fornecedores: estabelecimento de controles de segurança para gerenciar o risco cibernético de fornecedores e prestadores de serviços.

h. Conscientização: planos, tecnologias e controles utilizados para criar uma cultura de segurança da informação e assegurar que a força de trabalho possa reconhecer situações de risco e agir corretamente.

i. Arquitetura de segurança: gerenciamento dos processos, controles e tecnologias para a identificação de requisitos de segurança para os ativos cibernéticos e o desenho de controles apropriados para protegê-los.

j. Gestão do programa de segurança da informação: estabelecimento de programa que apoie na governança, no planejamento e na promoção das atividades de segurança cibernética, alinhando os objetivos de segurança aos objetivos da organização.

5 RESPONSABILIDADES

5.1. A segurança da informação é responsabilidade de cada empregado, terceiro, fornecedor, consultor e parceiro, devendo cada um conhecer e compreender as diretrizes e princípios estabelecidos para o cumprimento desta Política e estarem comprometidos com a proteção adequada de informações e sistemas contra ameaças e riscos.

5.2. Todas as pessoas com acessos ao ambiente SALSEC devem participar de atividades de conscientização sobre esta Política, com a finalidade de mitigar

possíveis riscos de segurança, compreender as suas responsabilidades e seguir os procedimentos recomendados.

5.3. Todos os colaboradores devem comunicar à área de Segurança da Informação quaisquer descumprimentos da Política de Segurança da Informação e Segurança Cibernética.

5.4. Cabe à Liderança orientar todos sob sua coordenação sobre o conteúdo desta Política, instruções e demais diretrizes de segurança e assegurar o seu cumprimento.

5.5. Cabe ao Comitê de Privacidade, Proteção de Dados e Segurança Cibernética avaliar e monitorar periodicamente as ações de segurança cibernética e segurança da informação, garantir recursos para a execução das atividades e apoiar as ações de promoção dessa Política.

6 DISPOSIÇÕES FINAIS

6.1. A presente Política de Segurança da Informação entrará em vigor na data da sua aprovação pelo Conselho de Administração, devendo ser atualizada quando algum fato relevante ou evento ocorrer que motive a sua revisão ou conforme análise e decisão do Comitê de Privacidade, Proteção de Dados e Segurança Cibernética.

6.2. As infrações a esta Política e aos seus documentos relacionados serão consideradas atos de desobediência, sujeitos à aplicação de sanções administrativas diretas e ainda aquelas previstas em legislação vigente.